Full Linear Integer Inequality Characterization of Sets over $\mathbb{Z}_2^n$

Xiutao Feng[1]✉, Yu Tian[1,2], Yongxing Wang[1,2], Shengyuan Xu[1,2], and Anpeng Zhang[1,2]

[1] Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences;
[2] University of Chinese Academy of Sciences
fengxt@amss.ac.cn

Abstract. In recent years, mixed integer linear programming (MILP, in short) is widely used to search differential characteristics and linear approximations with high probability and gradually becomes a powerful tool of automated cryptanalysis in symmetric ciphers. A key problem in the MILP method is how to fully characterize a set $S \subseteq \{0,1\}^n$ with as few linear integer inequalities L as possible, which is called a full linear integer inequality characterization (FLIIC, in short) problem. In this work we establish a complete theory to solve a best solution of a FLIIC problem. Specifically, we start from plain sets which can be characterized by exactly one linear integer inequality, and give their essential properties, including type, sparsity, degeneration, order, minimal and maximal element, norm and its bound, etc, and a sufficient and necessary condition characterizing them. Based on these essential properties, we further provide an algorithm for solving a FLIIC problem with S, which can produce all minimal plain closures (MPC, in short) of S and output a best FLIIC theoretically. Our algorithm is very efficient and practical, which can output the MPCs of S of dimension no more than 18. For example, all MPCs of the AES S-box are got within 32 seconds in our personal workstation. As results, we give the MPCs of many S-boxes used in block ciphers of size no more than 9×9 and their FLIIC solutions. To the best of our knowledge, it is the first time to give their all MPCs, and our all FLIIC solutions are the best-known results at present. In particular, our FLIIC solutions in the higher dimensional case are far better than the previous results, for example, we get a solution of the AES S-box only containing 2372 inequalities.

Keywords: Automated cryptanalysis · Mixed integer linear programming · Full linear integer inequality characterization · Plain set · Minimal closure

1 Introduction

Mixed integer linear programming (MILP, in short) is an important problem in operations research, which can be formally stated as follows: Given $A \in$

$\mathbb{R}^{m\times n}, b \in \mathbb{R}^m$ and $c_1, \cdots, c_n \in \mathbb{R}$, find an $x \in \mathbb{Z}^k \times \mathbb{R}^{n-k} \subseteq \mathbb{R}^n$ such that the linear function $c_1x_1 + c_2x_2 + \cdots + c_nx_n$ is minimized (or maximized) with respect to the linear constraints $Ax \leq b$, where $\mathbb{R}$ and $\mathbb{Z}$ are the sets of all real numbers and integers respectively. An MILP problem usually consists of three parts: variables, an objective function and constraints. There are several solvers to solve MILP problems such as Gurobi[Opt20], Cplex [Cpl09] and Minisat[ES03].

Differential analysis [BS91] and linear analysis [Mat93] are two of the most important cryptanalysis in block ciphers, and several useful techniques have been developed based on them, such as truncated differential attack [Knu94], related-key differential attack [Bih94], impossible differential attack [BBS99] and zero correlation attack [BR11]. In recent years, automated search algorithms for differential characteristics and linear approximations have gained considerable attention. The MILP-based method is the most used one among them, which was first introduced by Mouha *et al.* to search the minimal number of active S-boxes in differential analysis and linear analysis [MWGP11]. Later Sun *et al.* [SHW+14] described the differential property of an S-box with linear inequalities to search (related-key) differential characteristics automatically for bit-oriented block ciphers. Following that, the MILP method got considerable attention and was further applied to other cryptanalysis algorithms. In [FWG+16], Fu *et al.* searched differential and linear characteristics for ARX ciphers. Xiang *et al.* [XZBL16] searched integral distinguishers by translating the propagation of division property into an MILP problem. Zero-correlation distinguishers were searched in [TSK+16]. And in [ST17], some new impossible differential distinguishers were found by MILP techniques. In addition, a new MILP model was developed to consider the effect of the ladder switch technique when combining two short differential trails into boomerang or rectangle attacks [CHP+17]. By modeling the division trails with MILP language, the superpoly could be recovered in cube attacks [TIHM18].

1.1 Related Works

Mouha *et al.* [MWGP11] first applied the MILP method to automated search algorithms for differential cryptanalysis. A key problem of constructing an MILP model is to fully characterize a given set $S \subseteq \{0,1\}^n$ with linear integer inequalities. Mouha *et al.* characterized a specific set for $n = 3$ with dummy variables. Later, researchers focus on characterizing sets for $n \leq 16$ without dummy variables. Generally speaking, there are two steps to solve this problem: First produce abundant high quality linear inequalities L; Second choose as few linear inequalities L' from L as possible and expect that the solution set of them on $\{0,1\}^n$ just covers S.

In [SHW+14], Sun *et al.* computed the H-representation of the convex hull of S with a mathematical software SAGE [Dev20]. They first got L based on the H-representation and some logic conditions, and then applied a greedy algorithm to choose L'. However, their method became impractical when $n \geq 13$ due to the high time complexity of the H-representation computation. For $n \leq 16$, Abdelkhalek *et al.* [AST+17] converted the problem of finding L' into a problem

of minimizing the product-of-sum representation of Boolean functions and solved it with Quine-McCluskey algorithm [Qui52] or Espresso algorithm [BHMSV84]. A disadvantage of their method was that the solution L' they found usually contained too many linear inequalities, and another is to not guarantee that the number of linear inequalities in L' is minimal. In response to such a problem, Todo and Sasaki [ST17] proposed an MILP model to choose L' for a given set L. Their MILP model could help users obtain the minimal number of linear inequalities from L for $n \leq 10$. For $n > 10$, they usually got a better solution whose size was relatively small.

Afterwards, researchers tended to get a better L. In [LWZZ19], based on the relationship between coefficients of linear inequalities and the corresponding points in S, Li *et al.* proposed a new way to obtain L for $S \subseteq \{0,1\}^n$ from a lower dimensional case $S_{low} \subseteq \{0,1\}^{n-1}$. This method depended on previous methods and was suitable for a bit larger n. Boura *et al.* [BC20] further improved the results of previous works by means of algebraic and geometrical methods. For $n \leq 10$, they could get a potentially better L' from a given set of linear inequalities L by adding up some inequalities in L. For larger n, they explored a new structure of points in $\{0,1\}^n \setminus S$ that could be cut by the same inequality and got some better results.

We notice that Aleksei [Udo21] and Yao [Sun21] also studied properties of S that can be characterized by only one linear inequality [3], but there are many differences in ideas, methods and conclusions from ours, and a detail comparison will be provided in subsection 5.3.

1.2 Our Contributions

For a given subset S of $\{0,1\}^n$, L is a set of linear integer inequalities such that the solution set of L on $\{0,1\}^n$ is S exactly. We call L a full linear integer inequality characterization (FLIIC, in short) of S. Denote by $|L|$ the number of inequalities in L. Our goal is to find an L such that $|L|$ is as small as possible. Our main contribution is to establish a complete theory of solving a best solution of the above problem.

Firstly, we introduce an undirected graph of S and give a bound of $|L|$ based on graph theory, that is, $\mathcal{B}(G_n(\overline{S})) \leq |L| \leq |\overline{S}|$, where $\overline{S}$ is the complementary set of S in $\{0,1\}^n$, and $\mathcal{B}(G_n(\overline{S}))$ is the number of connected branches of $G_n(\overline{S})$.

Secondly, we focus on plain sets, which can be characterized by a single linear inequality l, and present their essential properties, including type, sparsity, degeneration, order, minimal and maximal element, norm and its bound, etc. And then we give a sufficient and necessary condition characterizing a plain set. Based on the above knowledge, we further provide an algorithm for solving a FLIIC problem with S, which can produce all minimal plain closures (MPC,

[3] Here it should be mentioned that our work was indeed independent with the above two works. In Sept 2021, we submitted it to EUROCRYPT 2022 and was rejected. Later we added some experimental data on high dimensional S-boxes and impossible differentials according to reviewers's comments.

in short) of S and output a best FLIIC theoretically. Our algorithm is very efficient and practical, which can output the MPCs of S of dimension no more than 18. For example, all MPCs of the AES S-box are got within 32 seconds in our workstation (DELL T640, 2 CPUs, 28 cores, 512G memory).

Finally, we apply our algorithm to many S-boxes used in block ciphers, and the exact number of closures and the computation time are listed in 1, and some results and comparisons with previous works are shown in Table 2. To the best of our knowledge, it is the first time to give their all MPCs, and our all FLIIC solutions are the best-known results at present.

Table 1. Number of all minimal closures of S-boxes and their computation times

S-box \ Methods		#Poss/#Imposs	#Minimal Closures	Times
4 bits	SKINNY64	97/159	704	$< 10^{-6}$ s
	RECTANGLE	97/159	1033	$< 10^{-6}$ s
	LBlock S0	97/159	737	$< 10^{-6}$ s
	LBlock S1	97/159	737	$< 10^{-6}$ s
	LBlock S2	97/159	737	$< 10^{-6}$ s
	PICCOLO	97/159	704	$< 10^{-6}$ s
	Serpent S6	97/159	464	$< 10^{-6}$ s
	GIFT	99/157	723	$< 10^{-6}$ s
	Present	97/159	464	$< 10^{-6}$ s
	Klein	106/150	370	$< 10^{-6}$ s
	Prince	106/150	330	$< 10^{-6}$ s
	Pride	97/159	694	$< 10^{-6}$ s
	FBC	97/159	921	$< 10^{-6}$ s
	Minalpher	106/150	322	$< 10^{-6}$ s
	Pyjamask	97/159	642	$< 10^{-6}$ s
	Noekeon	103/153	372	$< 10^{-6}$ s
	Panda	106/150	333	$< 10^{-6}$ s
	KNOT	97/159	1033	$< 10^{-6}$ s
	Elephant	97/159	631	$< 10^{-6}$ s
	SC2000-4	103/153	480	$< 10^{-6}$ s
	SC2000-4 Inv	103/153	480	$< 10^{-6}$ s
	EnocoroS4	103/153	480	$< 10^{-6}$ s
5 bits	KECCAK	317/707	95079	5.00 s
	Ascon	317/707	46765	0.4097 s
	FIDES-5	497/527	2163	0.0029 s
	SC2000-5	497/527	1790	$< 10^{-6}$ s
	DryGASCON128	317/707	46754	0.435 s
	Shamash	497/527	4637	0.0278 s
	Sycon	317/707	46746	0.433 s
6 bits	APN-6	2017/2079	31975	1 s
	FIDES-6	2017/2079	14359	0.0865 s
	SC2000-6	1954/2142	14896	0.0448 s
7 bits	WAGE	6361/10023	1312603	4m 18 s
	MISTY	8129/8255	77234	1 s
	Kasumi	8129/8255	77230	1 s
8 bits	AES	32386/33150	609962	32 s
	SMS4	32386/33150	626742	1 m 13 s
	ZUC S1	32386/33150	619751	51 s
	SNOW3G	25862/39674	3955092	45 m 59 s
	Camellia	32386/33150	632121	24 s

[1] The time column represents the running time of Algorithm 4;
[2] The #Poss (#Imposs) represents the number of the possible patterns(impossible patterns);

Table 2. Number of inequalities to model differential transitions for various S-boxes

S-box \ Methods		[SHW+14]	[ST17]	[LWZZ19]	[BC20]	[Udo21]	**Ours**
4 bits	SKINNY64	-	21	-	16	14	**14**
	RECTANGLE	-	-	-	17	15	**15**
	LBlock S0	28	24	-	17	-	**15**
	LBlock S1	27	24	-	17	-	**15**
	LBlock S2	27	24	-	17	-	**15**
	PICCOLO	23	21	-	16	14	**14**
	Serpent S6	22	-	-	17	-	**14**
	GIFT	-	-	-	17	16	**16**
	Present	22	21	-	17	16	**16**
	Klein	22	21	-	19	18	**18**
	Prince	26	22	-	19	18	**18**
	Pride	-	-	-	16	16	**16**
	FBC	-	-	-	16	-	**15**
	Minalpher	-	22	-	19	-	**18**
	Pyjamask	-	-	-	-	-	**15**
	Noekeon	-	-	-	-	-	**18**
	Panda	-	-	-	-	-	**20**
	KNOT	-	-	-	-	-	**15**
	Elephant	-	-	-	-	-	**17**
	SC2000-4	-	-	-	-	-	**19**
	SC2000-4 Inv	-	-	-	-	-	**19**
	EnocoroS4	-	-	-	-	-	**18**
5 bits	KECCAK	-	-	-	34	-	**26**
	Ascon	-	-	-	32	27	**27**
	FIDES-5	-	-	-	64	57	**57**
	SC2000-5	-	-	-	66	60	**60**
	DryGASCON128	-	-	-	-	-	**27**
	Shamash	-	-	-	-	-	**66**
	Sycon	-	-	-	-	-	**27**
6 bits	APN-6	-	-	-	167	145	**145**
	FIDES-6	-	-	-	180	162-166	162-**165**
	SC2000-6	-	-	-	218	188-205	189-**200**
7 bits	WAGE	-	-	-	-	-	459-**558**
	MISTY-7	-	-	-	-	-	619-**693**
	Kasumi	-	-	-	-	-	619-**693**
8 bits	AES	-	8302	< 4000	2882	2008-2699	2008-**2372**
	SKINNY128	-	372	-	302	not feasible	**172**
	SMS4	-	-	4146	-	-	2015-**2390**
	ZUC S0	-	-	-	-	-	**1661**
	ZUC S1	-	-	-	-	-	2005-**2364**
	SNOW3G	-	-	-	-	-	1537-**2036**
	Camellia	-	-	-	-	-	2019-**2387**
9 bits	MISTY-9	-	-	9431	-	-	**5720**
	DryGASCON256	-	-	-	-	-	**1521**

1.3 Organization

The rest of the paper is organized as follows: Some preliminaries and notations are given in Section 2. In Section 3, we discuss a FLIIC from the viewpoint of graph theory and give a bound of its characterization cardinality. In Section 4, we study some essential properties of plain sets, including type, sparsity, degeneration, order, minimal or maximal elements, norm and its bound, etc. Based on these properties, we obtain a sufficient and necessary condition of a plain set. In Section 5, to characterize an arbitrary given set S efficiently, we discuss the plain closure of S and provide a new algorithm to get all the minimal plain closures of S, which can be applied to solve a FLIIC problem with S. Finally, in Section 6, the best FLIICs of differential properties of many S-boxes used in block ciphers are obtained along with the exact number of their minimal closures. Meanwhile, some experiments results of automated cryptanalysis which can reflect the improvement of efficiency are provided.

2 Notations and Preliminaries

In the section we give a brief overview of some notations and definitions. Table 3 lists parts of notations.

Table 3. The notations used throughout the paper

Notation	Description
n	A positive integer
$\mathbb{Z}_2$	The set $\{0,1\}$
$\mathbb{Z}_2^n$	The set of all n-tuples over $\mathbb{Z}_2$, i.e., $\{0,1\}^n$
$\mathbf{\Pi}_n$	The set of all subsets of $\mathbb{Z}_2^n$
$\mathbf{P}_n$	The set of all plain sets in $\mathbb{Z}_2^n$
$\|\cdot\|$	Norm
$\lvert\cdot\rvert$	Absolute value of an integer or cardinality of a set
$\lvert\cdot\rvert_c$	Characterization cardinality of a set
$x[i]$	The i-th bit of x
$wt(x)$	Hamming weight of x
e_i	An n-bit unit whose i-th element is 1 and others are 0
$x \oplus y$	Bitwise XOR between x and y
$d(x,y)$	Hamming distance between x and $y, x, y \in \mathbb{Z}_2^n$
S	A subset of $\mathbb{Z}_2^n$
$\overline{S}$	The complementary set of S in $\mathbb{Z}_2^n$
$l : \sum_{i=0}^{n-1} a_i x_i \geq b$	A linear inequality whose coefficients are integers
$(a_0, a_1, \cdots, a_{n-1}, b)$	The linear inequality $\sum_{i=0}^{n-1} a_i x_i \geq b$
$L = \{l_i \mid l_i : \sum_{j=0}^{n-1} a_{i,j} x_j \geq b_i\}$	A set of inequalities whose coefficients are integers

Here we first introduce the concept of full linear integer inequality characterization for an arbitrary given set $S \in \mathbf{\Pi}_n$.

Definition 1 (Full Linear Integer Inequality Characterization). *Let $S \in \mathbf{\Pi}_n$ and L be a set of linear integer inequalities:*

$$\begin{cases} a_{0,0}x_0 + a_{0,1}x_1 + \cdots + a_{0,n-1}x_{n-1} \geq b_0, \\ a_{1,0}x_0 + a_{1,1}x_1 + \cdots + a_{1,n-1}x_{n-1} \geq b_1, \\ \vdots \\ a_{m-1,0}x_0 + a_{m-1,1}x_1 + \cdots + a_{m-1,n-1}x_{n-1} \geq b_{m-1}. \end{cases} \tag{1}$$

L is called a full linear integer inequality characterization (FLIIC, in short) of S if the solution set of L on $\mathbb{Z}_2^n$ is S exactly. We also say L fully characterizes S.

For a given set $S \in \mathbf{\Pi}_n$, a natural question is whether its FLIIC exists. Before answering this question, we make conventions on the meaning of the symbols l and L for convenience. For a given linear inequality

$$l : \sum_{i=0}^{n-1} a_i x_i \geq b,$$

we will use an $(n+1)$-tuple $(a_0, a_1, \cdots, a_{n-1}, b)$ to represent it. At the same time, we still use l to denote its solution set on $\mathbb{Z}_2^n$ without confusion. Thus $\bar{l}$ means the complementary set of l in $\mathbb{Z}_2^n$ when it is viewed as a set, and the inequality $\sum_{i=0}^{n-1} a_i x_i < b$ as an inequality, that is, $\sum_{i=0}^{n-1} (-a_i) x_i \geq -b+1$. Define the norm $\| l \|$ of l as below:

$$\| l \| := \max\{|a_i|, |b|, 0 \leq i \leq n-1\}.$$

Similarly, let $L = \{l_i | 0 \leq i \leq m-1\}$, and we have $L = \bigcap_{i=0}^{m-1} l$ when L is viewed as a set. Particularly, if L has only one inequality l, we use l instead of L. The norm $\| L \|$ of L is defined as below:

$$\| L \| := \max\{\| l_i \| \ \big| \ 0 \leq i \leq m-1\}.$$

A toy example is given here to illustrate the above definitions.

Example 1. Let

$$S = \{000, 100, 101\}$$

be a subset of $\mathbb{Z}_2^3$. Then the complementary set of S is

$$\overline{S} = \{010, 001, 110, 011, 111\}.$$

Denote the following inequality set as L:

$$\begin{cases} x_0 - x_1 - x_2 \geq 0, \\ -x_0 - x_1 + x_2 \geq -1, \end{cases}$$

which contains two inequalities, denoted by l_1 and l_2 respectively. Consider the solution sets of l_1,l_2, we have:

$$l_1 = \{000, 100, 110, 101\}$$

and

$$l_2 = \{000, 100, 010, 001, 101, 011, 111\}.$$

Since $L = l_1 \cap l_2 = S$, thus L is a FLIIC of S with $\parallel L \parallel = 1$.

Next we prove the existence of the FLIIC of S.

Theorem 1 (Existence of the FLIIC). *For an arbitrary given set $S \in \mathbf{\Pi}_n$, there must exist a FLIIC L of S.*

Proof: If $S = \mathbb{Z}_2^n$, it is easy to check $x_0 \geq 0$ is a FLIIC of S. When $S \neq \mathbb{Z}_2^n$, we have $\overline{S} \neq \varnothing$. For $x, c \in \mathbb{Z}_2^n$, we have $x[i] \oplus c[i] = x[i](1 - c[i]) + c[i](1 - x[i])$. Denote

$$l_c : \sum_{i=0}^{n-1} [(1 - c[i])x_i + c[i](1 - x_i)] \geq 1.$$

Then we have $\overline{l_c} = \{c\}$. Therefore $L = \{l_c \mid c \in \overline{S}\}$ is a FLIIC of S. □

For a given set $S \in \mathbf{\Pi}_n$, we know the FLIIC of S always exists. Denote by $\mathcal{C}(S)$ all FLIICs of S. Obviously, for any $L \in \mathcal{C}(S)$ and a positive integer k, we have $kL \in \mathcal{C}(S)$, where $kL = \{kl \mid l \in L\}$:

$$\sum_{i=0}^{n-1} a_i x_i \geq b \Leftrightarrow k \sum_{i=0}^{n-1} a_i x_i \geq kb.$$

Thus we have $|\mathcal{C}(S)| = \infty$. In order to improve the efficiency of the MILP method, we expect that L chosen from $\mathcal{C}(S)$ satisfies that both $|L|$ and $\parallel L \parallel$ are as small as possible. Therefore we introduce two concepts of the characterization cardinality and norm of S.

Definition 2 (The Characterization Cardinality and Norm of Set). *For a set $S \in \mathbf{\Pi}_n$, its characterization cardinality, denoted by $|S|_c$, is defined as the minimal cardinality of all FLIICs of S:*

$$|S|_c = \min\{|L| \mid L \in \mathcal{C}(S)\}$$

and its norm, denoted by $\|S\|$, as the minimal norm of all FLIICs with characterization $|S|_c$ of S:

$$\parallel S \parallel = \min\{\parallel L \parallel \mid |L| = |S|_c, L \in \mathcal{C}(S)\}.$$

To describe the FLIICs with minimal cardinality and norm, we introduce the definition of best FLIIC.

Definition 3 (Best FLIIC). *For $S \in \mathbf{\Pi}_n$ and $L \in \mathcal{C}(S)$, we say L is a best FLIIC of S if $|L| = |S|_c$ and $\parallel L \parallel = \parallel S \parallel$.*

According to the definition, there might be more than one best FLIICs, while they have the same cardinality and norm.

Example 2. Review Example 1 mentioned above. It is easy to check that S is also the solution set of

$$l : x_0 - 2x_1 - x_2 \geq 0,$$

i.e., $L = l = S$. Hence $|S|_c = 1$. Further one can verify that l is a best FLIIC of S.

For a random set $S \in \mathbf{\Pi}_n$, it is NP-hard to find a best FLIIC of S. In this paper our major work is to find a best FLIIC efficiently of S when n is not too big. To do it, we first consider the simplest case $|S|_c = 1$, that is, the set can be fully characterized by only one linear integer inequality.

Definition 4 (Plain Set). *For $S \in \mathbf{\Pi}_n$, we say S is plain if $|S|_c = 1$.*

Denote by $\mathbf{P}_n$ the set of all plain sets in $\mathbf{\Pi}_n$. Obviously, $\varnothing, \mathbb{Z}_2^n \in \mathbf{P}_n$. We say $\varnothing$ and $\mathbb{Z}_2^n$ are trivial, and $S \in \mathbf{P}_n \backslash \{\varnothing, \mathbb{Z}_2^n\}$ is non-trivial.

Proposition 1. *If $S \in \mathbf{P}_n$, then $\overline{S} \in \mathbf{P}_n$.*

Proof: Let $\{l\} \in \mathcal{C}(S)$. Then $\{\bar{l}\} \in \mathcal{C}(\overline{S})$. So $\overline{S} \in \mathbf{P}_n$. □

Below we introduce the concept of shift, which will play an important role in our discussion.

Definition 5 (Shift). *For $c \in \mathbb{Z}_2^n$, denote*

$$c \oplus S = \{c \oplus x \mid x \in S\} \tag{2}$$

and call $c \oplus S$ the c-shift of S. Similarly, for $l : \sum_{i=0}^{n-1} a_i x_i \geq b$ and $c \in \mathbb{Z}_2^n$, denote

$$l^c : \sum_{i=0}^{n-1} a_i[c_i(1 - x_i) + x_i(1 - c_i)] \geq b \tag{3}$$

and call l^c the c-shift of l.

Let L be a group of linear inequalities. We denote

$$L^c = \{l^c \mid l \in L\}. \tag{4}$$

As for the shift, we have the following conclusions.

Lemma 1. *For any $S \in \mathbf{P}_n$, $\{l\} \in \mathcal{C}(S)$ and $c \in \mathbb{Z}_2^n$, we have $\{l^c\} \in \mathcal{C}(c \oplus S)$.*

Proof: Set $l : \sum_{i=0}^{n-1} a_i x_i \geq b$. For $c \in \mathbb{Z}_2^n$ and $x \in c \oplus S$,

$$x[i] \oplus c[i] = c[i](1 - x_i) + x_i(1 - c[i])$$

always holds. Thus, for $c \oplus x \in S$, we have

$$\sum_{i=0}^{n-1} a_i(x[i] \oplus c[i]) \geq b$$

$$\Updownarrow$$

$$\sum_{i=0}^{n-1} a_i[c[i](1-x[i]) + x[i](1-c[i])] \geq b.$$

So $l^c = c \oplus S$, that is, $\{l^c\} \in \mathcal{C}(c \oplus S)$. □

Theorem 2 (Shift Theorem). *For any $S \in \mathbf{\Pi}_n$, $L \in \mathcal{C}(S)$ and $c \in \mathbb{Z}_2^n$, we have $L^c \in \mathcal{C}(c \oplus S)$.*

Proof: By Lemma 1, we have

$$L^c = \bigcap_{l \in L} l^c = \bigcap_{l \in L} (c \oplus l) = c \oplus \bigcap_{l \in L} l = c \oplus S.$$

The conclusion follows. □

Corollary 1. *For any $S \in \mathbf{P}_n$ and $c \in \mathbb{Z}_2^n$, we have $c \oplus S \in \mathbf{P}_n$.*

Example 3. Take $S = \{000, 100, 101\} \subset \mathbb{Z}_2^3$, $l : x_0 - 2x_1 - x_2 \geq 0$ and $c = 101$. By the definition of shift, we have

$$c \oplus S = \{101, 001, 000\}$$

and

$$l^c : (1 - x_0) - 2x_1 - (1 - x_2) \geq 0,$$

i.e.,

$$l^c : -x_0 - 2x_1 + x_2 \geq 0.$$

It is easy to check that l^c fully characterizes $c \oplus S$, hence $c \oplus S$ is also plain.

3 Graph Structures of Sets

In the section we will discuss some properties of plain sets from the viewpoint of graph theory. For any non-empty $S \in \mathbf{\Pi}_n$, we can construct an undirected graph $G_n(S)$ as below:

1. The vertex set is just S;
2. There is an edge between x and y if and only if $d(x, y) = 1$ for $x, y \in S$.

When $S = \mathbb{Z}_2^n$, we rewrite $G_n(\mathbb{Z}_2^n)$ as G_n simply. For a given set $S \in \mathbf{\Pi}_n$, finding its FLIIC is equivalent to finding a set of linear inequalities $L = \{l_i\}_{1 \leq i \leq m}$ such that $\overline{S} = \bigcup_{1 \leq i \leq m} \overline{l_i}$. We notice that the connectivity of $G_n(\overline{S})$ is an important parameter to determine a set $L \in \mathcal{C}(S)$ and the lower bound of $|S|_c$. Here are some definitions and conclusions about the connectivity of $G_n(S)$.

Definition 6. *For $x, y \in \mathbb{Z}_2^n$, we say $x = p_0 \to p_1 \to \cdots \to p_t = y$ is a path linking x and y if $p_0, p_1, \cdots, p_t \in \mathbb{Z}_2^n$ and $d(p_i, p_{i+1}) = 1$ for $i = 0, 1, \cdots, t-1$.*

Lemma 2. *Let $S \in \mathbf{P}_n$ with $|S| \geq 2$. Then for two arbitrary distinct vertexes $x, y \in S$, there is always a path $x = p_0 \to p_1 \to \cdots \to p_t = y$, where $p_i \in S$ for $i = 0, 1, \cdots, t$.*

Proof: Suppose $\sum_{i=0}^{n-1} a_i x_i \geq b$ fully characterizes S. Denote $f(x) = \sum_{i=0}^{n-1} a_i x[i]$ for any $x \in \mathbb{Z}_2^n$. Let

$$W = \{i \mid x[i] \neq y[i], i = 0, 1, \cdots, n-1\},$$
$$I = \{i \in W \mid x[i] = 1, a_i < 0 \text{ or } x[i] = 0, a_i \geq 0\} = \{i_1, i_2, \cdots, i_r\},$$
$$J = \{j \in W \mid x[j] = 1, a_j \geq 0 \text{ or } x[j] = 0, a_j < 0\} = \{j_1, j_2, \cdots, j_s\}.$$

Denote $p_0 = x$. Construct $p_k \in \mathbb{Z}_2^n, k = 1, 2, \cdots, r$ as follows:

$$p_k = p_{k-1} \oplus e_{i_k}, i_k \in I$$

and $p_{r+k} \in \mathbb{Z}_2^n, k = 1, 2, \cdots, s$ as follows:

$$p_{r+k} = p_{r+k-1} \oplus e_{j_k}, j_k \in J.$$

Then we have $y = p_{r+s}$ and $d(p_i, p_{i+1}) = 1, i = 0, 1, \cdots, s+r-1$.

By the definitions of I and J, we have

$$f(p_r) \geq \cdots \geq f(p_1) \geq f(p_0) = f(x) \geq b,$$
$$f(p_{r+1}) \geq f(p_{r+2}) \geq \cdots \geq f(p_{r+s}) = f(y) \geq b.$$

Therefore, $p_i \in S, i = 1, 2, \cdots, r+s-1$. The conclusion follows. □

Proposition 2. *For $S \in \mathbf{P}_n$, $G_n(S)$ and $G_n(\overline{S})$ are connected.*

Proof: The conclusion follows directly from Lemma 2 and Proposition 1. □

For any $S \in \mathbf{\Pi}_n$, denote by $\mathcal{B}(G_n(S))$ the number of connected branches of $G_n(S)$, which gives a lower bound of the characterization cardinality of S.

Proposition 3. *For $S \in \mathbf{\Pi}_n$, we have*

$$\mathcal{B}(G_n(\overline{S})) \leq |S|_c \leq |\overline{S}|. \tag{5}$$

Proof: By Theorem 1, there exists an $L \in \mathcal{C}(S)$ such that $|L| = |\overline{S}|$, which indicates $|S|_c \leq |\overline{S}|$.

Suppose $G_n(\overline{S})$ has k distinct connected branches $G_n(\overline{S}_1), \cdots, G_n(\overline{S}_k)$. For any $L \in \mathcal{C}(S)$, we have $\overline{S} = \bigcup_{l \in L} \bar{l}$. Note that $G_n(\bar{l})$ is connected for any $l \in L$, thus there exists $1 \leq i \leq k$ such that $\bar{l} \subseteq \overline{S}_i$. It implies that L has at least k inequalities, that is, $\mathcal{B}(G_n(\overline{S})) \leq |S|_c$. □

Next we give a common case on the characterization of the exclusive-or operation.

Proposition 4. *Let $b \in \mathbb{Z}_2$ and*

$$S_b = \{x \in \mathbb{Z}_2^n \mid x[0] \oplus x[1] \oplus \cdots \oplus x[n-1] = b\}.$$

Then $|S_b|_c = 2^{n-1}$.

Proof: The conclusion follows from $|\overline{S_b}| = 2^{n-1}$ and two arbitrary vertexes in $G_n(\overline{S_b})$ are not connected, that is, $\mathcal{B}(G_n(\overline{S_b})) = 2^{n-1}$. □

Remark 1. The same conclusion is obtained from a different point of view in [BC20].

4 Essential Properties of Plain Sets

In the section we will further explore some essential properties of plain sets, including type, sparsity, degeneration, order, minimal or maximal elements, norm and its bound, and so on. Based on these properties, we further propose the sufficient and necessary condition for the plain set.

4.1 Type, Sparsity and Degeneration

Here we start from the type of a linear inequality l.

Definition 7 (Type). *For a given linear inequality l:*

$$a_0x_0 + a_1x_1 + \cdots + a_{n-1}x_{n-1} \geq b,$$

the type of l is defined as an n-bit string $\lambda \in \{'-','+','0'\}^n$, where

$$\lambda[i] = \begin{cases} '+' & \text{if } a_i > 0; \\ '-' & \text{if } a_i < 0; \\ '0' & \text{if } a_i = 0. \end{cases} \tag{6}$$

Obviously, there are 3^n possible types of inequalities with n variables. For a given set $S \in \mathbf{\Pi}_n$, denote

$$\begin{aligned} \overline{S}_i^+ &= \{x \in \overline{S} | x[i] = 0,\ x \oplus e_i \in S\}, \\ \overline{S}_i^- &= \{x \in \overline{S} | x[i] = 1,\ x \oplus e_i \in S\}, \\ \overline{S}_i &= \{x \in \overline{S} | x \oplus e_i \in S\} = \overline{S}_i^+ \cup \overline{S}_i^-. \end{aligned} \tag{7}$$

As for plain sets, the following lemma explores the relationship between the sets defined above and signs of coefficients of their FLIICs.

Lemma 3. *Suppose $\mathbb{Z}_2^n \neq S \in \mathbf{P}_n$, $\{l = (a_0, a_1, \cdots, a_{n-1}, b)\} \in \mathcal{C}(S)$. Then for $0 \leq i \leq n-1$, the following properties always hold:*

1. *$\overline{S}_i^+$ and $\overline{S}_i^-$ can not be non-empty at the same time;*

2. *If* $\overline{S}_i^+ \neq \varnothing$, *then* $a_i > 0$;
3. *If* $\overline{S}_i^- \neq \varnothing$, *then* $a_i < 0$;
4. *If* $a_i = 0$, *then* $\overline{S}_i = \varnothing$.

Proof: We first prove Item 2. Suppose $\overline{S}_i^+ \neq \varnothing$, then there exists $x \in \overline{S}_i^+$ such that $x \in \bar{l}$ and $x[i] = 0$, meanwhile, $x \oplus e_i \in l$. Hence we have $a_i + \sum_{j \neq i} a_j x_j \geq b$ and $\sum_{j \neq i} a_j x_j < b$, which imply $a_i > 0$. Similarly we can prove Item 3. Note that at most one of two cases $a_i > 0$ and $a_i < 0$ holds, thus $\overline{S}_i^+$ and $\overline{S}_i^-$ cannot be non-empty at the same time. Finally, when $a_i = 0$, neither of the above situations happens, i.e., $\overline{S}_i^+ = \varnothing = \overline{S}_i^-$, hence $\overline{S}_i = \overline{S}_i^+ \cup \overline{S}_i^- = \varnothing$. □

For $S \in \mathbf{P}_n$ with $\overline{S}_i = \varnothing$ for some $0 \leq i \leq n-1$, if

$$\{l = (a_0, a_1, \cdots, a_{i-1}, a_i, a_{i+1}, \cdots, a_{n-1}, b)\} \in \mathcal{C}(S)$$

with $a_i \neq 0$, we notice that $l' = (a_0, a_1, \cdots, a_{i-1}, 0, a_{i+1}, \cdots, a_{n-1}, b)$ is also a FLIIC of S. This is because: if $x \in \overline{S}$, then $x \oplus e_i \in \overline{S}$ according to $\overline{S}_i^+ = \varnothing$; if $x \oplus e_i \in \overline{S}$, then $x \in \overline{S}$ according to $\overline{S}_i^- = \varnothing$. In summary, for all $x \in \mathbb{Z}_2^n$, $x \in S$ if and only if $x \oplus e_i \in S$. Therefore we always set $a_i = 0$ when $\overline{S}_i = \varnothing$ in the rest of the paper. So all statements in Lemma 3 turn into sufficient and necessary conditions.

Theorem 3 (Type Theroem). *Suppose* $\mathbb{Z}_2^n \neq S \in \mathbf{P}_n$ *and*

$$\{l = (a_0, a_1, \cdots, a_{n-1}, b)\} \in \mathcal{C}(S)$$

such that $a_i = 0$ *if* $\overline{S}_i = \varnothing$ *for some* i*'s. Then, for* $0 \leq i \leq n-1$, *the following properties always hold:*

1. $\overline{S}_i^+$ *and* $\overline{S}_i^-$ *cannot be non-empty at the same time;*
2. $\overline{S}_i^+ \neq \varnothing$ *if and only if* $a_i > 0$;
3. $\overline{S}_i^- \neq \varnothing$, *if and only if* $a_i < 0$.

The proof of Theorem 3 is similar to that of Lemma 3, and we do not repeat it. By the Type Theorem, we know that for a given plain set S, the type of its FLIIC l is uniquely determined by S itself. In this case we also call it the type of S, denoted by $\lambda(S)$. Below we further introduce the concepts of sparsity and degeneration of plain sets.

Definition 8 (Sparsity). *Let* $S \in \mathbf{P}_n$ *and* $\lambda = \lambda(S)$. *The sparsity of* S, *denoted by* $\chi(S)$, *is defined as the number of zero bits in its type* λ, *i.e.,*

$$\chi(S) := \#\{i | \lambda[i] =' 0', 0 \leq i \leq n-1\}. \tag{8}$$

Definition 9 (Degenerate). *For a plain set* $S \in \mathbf{P}_n$, *we call* S *to be degenerate if* $\chi(S) > 0$; *otherwise,* S *is non-degenerate if* $\chi(S) = 0$.

In order to distinguish with the secondary degeneration introduced in Section 5, we call it the first degeneration later. Denote by $\mathbf{P}_n^*$ the set of all non-degenerate plain sets, i.e.,

$$\mathbf{P}_n^* = \{S \in \mathbf{P}_n | \chi(S) = 0\}. \tag{9}$$

For a degenerate plain set S, suppose $\chi(S) = n' < n$ and l is a FLIIC of S, then l equivalently characterizes a set $S' \subseteq Z_2^{n-n'}$, where S' can be got by removing some bits from all $x \in S$ corresponding to $a_i = 0$. Thus we only focus on non-degenerate plain sets.

4.2 Order

In the section we mainly discuss the order of the plain set S.

Let $S \in \mathbf{P}_n$ and $\{l = (a_0, a_1, \cdots, a_{n-1}, b)\} \in \mathcal{C}(S)$. Notice that there exists a natural order among the coefficients a_i. In order to characterize such an order, we denote

$$\begin{aligned} \Gamma_i &:= \{x \in S \mid x[i] = 1\}, \\ \Gamma_{i,j} &:= \{x \oplus e_i \mid (x \in \Gamma_i) \wedge (x[j] = 0)\} \end{aligned} \tag{10}$$

for $0 \leq i \neq j \leq n-1$. As for $\Gamma_{i,j}$, we have the following conclusion:

Lemma 4. *Suppose $S \in \mathbf{P}_n$ and $(a_0, a_1, \cdots, a_{n-1}, b) \in \mathcal{C}(S)$. Then $\Gamma_{i,j} \subseteq \Gamma_{j,i}$ always holds if $a_i \leq a_j$. Especially, $\Gamma_{i,j} = \Gamma_{j,i}$ holds when $a_i = a_j$.*

Proof: Suppose $x \in \Gamma_{i,j}$, then $x[i] = x[j] = 0$ and $x \oplus e_i \in S$. Since $a_i \leq a_j$, we have

$$b \leq a_i + \sum_{k \neq i,j} a_k x[k] \leq a_j + \sum_{k \neq i,j} a_k x[k].$$

Thus $x \oplus e_j \in S$ holds, i.e., $x \in \Gamma_{j,i}$, which implies $\Gamma_{i,j} \subseteq \Gamma_{j,i}$. Suppose $a_i = a_j$. For any $x \in \mathbb{Z}_2^n$ with $x[i] = x[j] = 0$, $x \oplus e_i \in S$ if and only if $x \oplus e_j \in S$. Thus $\Gamma_{i,j} = \Gamma_{j,i}$. □

For $S \in \mathbf{P}_n$ with $\Gamma_{i,j} = \Gamma_{j,i}$ for some i and j, if

$$\{l = (a_0, a_1, \cdots, a_i, \cdots, a_j, \cdots, a_{n-1}, b)\} \in \mathcal{C}(S)$$

with $a_i \neq a_j$, we notice that $l' = (a_0, a_1, \cdots, a_i, \cdots, a_i, \cdots, a_{n-1}, b)$ is also a FLIIC of S. This is because: if $x \oplus e_j \in S$, then $x \oplus e_i \in S$ naturally holds; if $x \oplus e_i \in S$, then $x \in \Gamma_{i,j} = \Gamma_{j,i}$, i.e., $x \oplus e_j \in S$. In summary, $x \oplus e_i \in S$ if and only if $x \oplus e_j \in S$. Therefore we can always set $a_i = a_j$. Denote by $\mathbf{L}$ the set of all linear integer inequalities $l : (a_0, a_1, \cdots, a_{n-1}, b)$ such that $a_i = 0$ if $\bar{l}_i = \varnothing$ for some i's and $a_i = a_j$ if $\Gamma_{i,j} = \Gamma_{j,i}$ for some i's and j's. In this paper we mainly focus on linear integer inequalities in $\mathcal{L}$ and use them to fully characterize a given set S. For any $S \in \mathbf{\Pi}_n$, denote

$$\mathcal{C}^*(S) = \{L \in \mathcal{C}(S) \mid l \in L \wedge l \in \mathcal{L}\}. \tag{11}$$

Theorem 4 (Order Theorem). *Suppose* $S \in \mathbf{P}_n^*$ *and* $\{(a_0, a_1, \cdots, a_{n-1}, b)\} \in \mathcal{C}^*(S)$. *Then* $a_i < a_j$ *if and only if* $\Gamma_{i,j} \subset \Gamma_{j,i}$.

Proof: The necessity is directly indicated by Lemma 4. Suppose $\Gamma_{i,j} \subset \Gamma_{j,i}$, then $\exists x \in \mathbb{Z}_2^n$ with $x[i] = x[j] = 0$ such that $x \oplus e_j \in S$ and $x \oplus e_i \notin S$. Then we have

$$a_i + \sum_{k \neq i,j} a_k x[k] < b \leq a_j + \sum_{k \neq i,j} a_k x[k],$$

which implies $a_i < a_j$. So the conclusion holds. □

For a given set $S \in \mathbf{P}_n$, by the Order Theorem, S can derive a bit-level position permutation σ, where σ meets $a_{\sigma(i)} \leq a_{\sigma(j)}$ when $i < j$. Thus we can assume that there exists a default relationship of order :

$$a_0 \leq a_1 \leq \cdots \leq a_{n-1}.$$

Otherwise, we will act σ on S to make it hold.

Definition 10 (Regular Plain Set). *A non-degenerate plain set* S *is called a regular plain set if there exists a*

$$\{(a_0, a_1, \cdots, a_{n-1}, b)\} \in \mathcal{C}^*(S),$$

such that $1 \leq a_0 \leq a_1 \leq \cdots \leq a_{n-1}$.

Denote by $\mathbf{P}_{n,+}^*$ the set of all regular plain sets. For any $S \in \mathbf{P}_n^*$, we can always convert it into a regular plain set by the following two operations:

- **Type Shift**: Let $c \in Z_2^n$ such that

$$c[i] = \begin{cases} 0, \text{ if } \lambda[i] =' +'; \\ 1, \text{ if } \lambda[i] =' -', \end{cases}$$

  where $\lambda = \lambda(S)$. We act a shift c on S and call c the type vector of S. After the type shift c, all coefficients of the FLIICs of $S' = c \oplus S$ are positive.
- **Position Permutation**: Let σ be a position permutation derived by S'. Then all coefficients of the FLIICs of $S'' = \sigma(S')$ satisfy

$$1 \leq a_0 \leq a_2 \leq \cdots \leq a_{n-1}.$$

On the contrary, if we have a FLIIC l'' of S'', we first act the inverse σ^{-1} on l'' to get a FLIIC l' of S' and then a type shift c on l' to get a FLIIC l of S. Figure 1 illustrates the above procedure. Therefore we only consider a regular plain set S in the rest of the paper.

Let $x \in \mathbb{Z}_2^n$, denote by $\mathrm{supp}(x)$ the set of the positions of ones in the binary representation of x:

$$\mathrm{supp}(x) = \{i \mid x[i] = 1, 0 \leq i \leq n-1\},$$

which is called the support set of x. Below we introduce a partial order relation among elements in $\mathbb{Z}_2^n$.

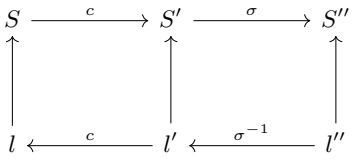

Fig. 1. Diagram of the type shift and the position permutation

Definition 11 (Weak Order). *For $x, y \in \mathbb{Z}_2^n$, we say $x \dot{\preceq} y$ if $supp(x) \subseteq supp(x)$.*

Definition 12 (Strong Order). *For $x, y \in \mathbb{Z}_2^n$, denote*

$$supp(x) = \{i \mid x[i] = 1, 0 \leq i \leq n-1\} = \{i_1, i_2, \cdots, i_s\},$$
$$supp(y) = \{j \mid y[j] = 1, 0 \leq j \leq n-1\} = \{j_1, j_2, \cdots, j_t\},$$

where s and t are positive integers, $i_1 < i_2 < \cdots < i_s$, $j_1 < j_2 < \cdots < j_t$. We say $x \preceq y$ if $s \leq t$ and $i_{s-k} \leq j_{t-k}$ for all $0 \leq k \leq s-1$. Further, we say $x \prec y$ if $x \preceq y$ and $x \neq y$.

Definition 13 (Ordered Set). *For any $S \in \mathbf{\Pi}_n$, S is called an ordered set if for any $x \in S$ and $x' \in \mathbb{Z}_2^n$, if $x \prec x'$, then $x' \in S$.*

The following proposition explores the relationship between an ordered set S and connectivity of the graph $G_n(S)$.

Proposition 5. *Let $S \in \mathbf{\Pi}_n$ be an ordered set. Then $G_n(S)$ is connected.*

Proof: For any given $x, y \in S$, denote

$$I = \{i \mid x[i] = 0, 0 \leq i \leq n-1\} = \{i_0, i_1, \cdots, i_{s-1}\},$$
$$J = \{j \mid y[j] = 0, 0 \leq j \leq n-1\} = \{j_0, j_1, \cdots, j_{t-1}\}.$$

Take $p_0 = x$, $p_{k+1} = p_k \oplus e_{i_k}$ $(k = 0, 1, \cdots, s-1)$ and $p_{s+k+1} = p_{s+k} \oplus e_{j_k}$ $(k = 0, 1, \cdots, t-1)$. Note that $p_{s+t} = y$ and $d(p_k, p_{k+1}) = 1$ $(0 \leq k \leq s+t-1)$, we have

$$x = p_0 \to p_1 \to \cdots \to p_s \to p_{s+1} \to \cdots \to p_{s+t} = y,$$

which implies that $G_n(S)$ is connected. □

It should be noted that there have been some similar works which consider points in $\mathbb{Z}_2^n$ from the perspective of order [Udo21] [Sun21]. We find that what they discussed was only the inclusion relationship among points in $\mathbb{Z}_2^n$, see Definition 11. They did not consider the relationship among coefficients of the corresponding inequality. For comparison, we call it a weak order and call the corresponding set to be a weakly ordered set. By Theorem 4, for any $S \in \mathbf{P}_n$, the order among coefficients of the inequalities $l \in \mathcal{C}^*(S)$ is completely determined. That is to say, an order we defined always exists for any $S \in \mathbf{P}_n$. Therefore the order we define is more essential and powerful than the weak order. The

following proposition shows that a weakly ordered set S can be characterized fully by the sets $\overline{S_i^-}$ $(i=0,1,\cdots,n-1)$. Since we do not discuss the weak order too much in this paper, its proof is omitted here.

Proposition 6. *Let $S \in \mathbf{\Pi}_n$. Then S is a weakly ordered set if and only if $\overline{S_i^-} = \varnothing$ for all $i \in \{0,\cdots,n-1\}$.*

4.3 Good Set

Finally we introduce the concept of good set, which can fully characterize a plain set.

Definition 14. *For $x,y,x',y' \in \mathbb{Z}_2^n$, we say $x\dot{+}x' = y\dot{+}y'$ if $x[i]+x'[i] = y[i]+y'[i]$ holds for $i=0,1,\cdots,n-1$, where $+$ means the common integer addition.*

This definition can be easily generalized to the form of sums of n terms.

Definition 15 (Good Set). *Let $S \in \mathbf{\Pi}_n$. S is good if it meets the following two conditions:*

1. ***Order Condition**: S is an ordered set;*
2. ***Consistent Condition**: There do not exist $2k$ elements $x_0,x_1,\cdots,x_{k-1} \in S$ and $y_0,y_1,\cdots,y_{k-1} \in \overline{S}$ such that $x_0\dot{+}x_1\dot{+}\cdots\dot{+}x_{k-1} = y_0\dot{+}y_1\dot{+}\cdots\dot{+}y_{k-1}$.*

Theorem 5 (Main Theorem). *$S \in \mathbf{P}_{n,+}^*$ if and only if S is good.*

Proof: The necessity is trivial since for any $2k$ elements $x_0,x_1,\cdots,x_{k-1} \in S$ and $y_0,y_1,\cdots,y_{k-1} \in \overline{S}$, we have

$$\sum_{j=0}^{k-1}\sum_{i=0}^{n-1} a_i y_j[i] < kb \le \sum_{j=0}^{k-1}\sum_{i=0}^{n-1} a_i x_j[i],$$

where $(a_0,a_1,\cdots,a_{n-1},b) \in \mathcal{C}(S)$, which implies

$$x_0\dot{+}x_1\dot{+}\cdots\dot{+}x_{k-1} \neq y_0\dot{+}y_1\dot{+}\cdots\dot{+}y_{k-1}.$$

Below we prove the sufficiency. Suppose $S \notin \mathbf{P}_{n,+}^*$, which means the inequality system:

$$\begin{cases} \sum\limits_{i=0}^{n-1} a_i x[i] \ge b, x \in S; \\ \sum\limits_{i=0}^{n-1} a_i y[i] < b, y \in \overline{S}; \\ 0 < a_0 \le a_1 \le \cdots \le a_{n-1}. \end{cases} \tag{12}$$

has no solution. From (12), there must exist a subsystem containing k elements $x_0,x_1,\cdots,x_{k-1} \in S$ and t elements $y_0,y_1,\cdots,y_{t-1} \in \overline{S}$ such that the contradiction

$$kb \le \sum_{j=0}^{k-1}\sum_{i=0}^{n-1} a_i x_j[i] \le \sum_{j=0}^{t-1}\sum_{i=0}^{n-1} a_i y_j[i] < tb$$

arises, where $k \geq t$. Here we assume that $k = t$ without a loss of generality. This is because: If $k > t$, we can choose another $k-t$ elements $y_t, \cdots, y_{k-1}$ arbitrarily from $\overline{S}$, the inequality

$$kb \leq \sum_{j=0}^{k-1}\sum_{i=0}^{n-1} a_i x_j[i] \leq \sum_{j=0}^{k-1}\sum_{i=0}^{n-1} a_i y_j[i] < kb$$

still holds. Note that

$$\sum_{i=0}^{n-1} a_i (\sum_{j=0}^{k-1} y_j[i] - \sum_{j=0}^{k-1} x_j[i]) > 0$$

always holds for all $0 < a_0 \leq a_1 \leq \cdots \leq a_{n-1}$, we check gradually for i from $n-1$ to 0 whether $\sum_{j=0}^{k-1} x_j[i] = \sum_{j=0}^{k-1} y_j[i]$ holds or not. If it is not, that is, $\sum_{j=0}^{k-1} x_j[i] < \sum_{j=0}^{k-1} y_j[i]$, since $\overline{S}$ is an ordered set, thus one can always choose some smaller y_j' from $\overline{S}$ instead of some y_j (Here we give preference to y_j with $y_j[i] = 1$ and $y_j[i-1] = 0$, and $y_j' = y_j + e_i + e_{i-1}$) such that it holds. It contradicts with the consistent condition of S. So $S \in \mathbf{P}^*_{n,+}$. □

4.4 Minimal and Maximal Element

In the section we will discuss the minimal and maximal elements of ordered sets and their properties.

Definition 16 (Minimal and Maximal Element). *Let $S \in \mathbf{\Pi}_n$ be an ordered set. For any $x \in S$, x is called a minimal element if $\nexists y \in S$ such that $y \prec x$, and a maximal element if $\nexists y \in S$ such that $x \prec y$.*

For a given ordered set S, denoted by $S_{\min}$ and $S_{\max}$ the set of all minimal elements and maximal elements in S respectively. Now we consider how to get a FLIIC l fast for a given set $S \in \mathbf{P}^*_{n,+}$. Suppose $(a_0, a_1, \cdots, a_{n-1}, b) \in \mathcal{C}(S)$, and denote

$$f(x) = \sum_{i=0}^{n-1} a_i x[i]. \tag{13}$$

A common method is to solve a group of linear inequalities with $(n+1)$ variables and 2^n inequalities, where $f(x) \geq b$ for any $x \in S$ and $f(x) < b$ for any $x \in \overline{S}$. Note that for any $x, y \in \mathbb{Z}_2^n$, if $x \prec y$, then we have $f(x) \leq f(y)$, that is, if $f(x) \geq b$ and $x \prec y$, then $f(y) \geq b$ always holds, and if $f(y) < b$ and $x \prec y$, then $f(x) < b$ always holds. Hence we only need to solve a simplified group of linear inequalities with $(n+1)$ variables and $(|S_{\min}| + |\overline{S}_{\max}|)$ inequalities, where $f(x) \geq b$ for any $x \in S_{\min}$ and $f(x) < b$ for any $x \in \overline{S}_{\max}$. Algorithm 1 gives all details of getting a best FLIIC fast for a given set $S \in \mathbf{P}^*_{n,+}$.

Below we simplly discuss the upper bound of $|S_{\min}| + |\overline{S}_{\max}|$. Denote $M_n = \max\{|S_{\max}| \mid S \in \mathit{\Pi}_n\}$. Referring to the paper [Inc21], one can find that M_n

Algorithm 1 Get a best FLIIC l of S

Input: A regular plain set $S \in \mathbf{P}^*_{n,+}$
Output: A FLIIC l with $\| l \| = \| S \|$

1: Compute $S_{\min}$ and $\overline{S}_{\max}$;
2: Construct the MILP model:
   - For all $x \in S_{\min}$, add constrains $\sum_{i=0}^{n-1} a_i x[i] \geq b$;
   - For all $x \in \overline{S}_{\max}$, add constrains $\sum_{i=0}^{n-1} a_i x[i] < b$;
   - Add constrains $1 \leq a_0 \leq a_1 \leq \cdots \leq a_{n-1} \leq b$;
   - Set Objective function : $\min b$;
3: Use Gurobi to solve the above problem and get a solution l;
4: **return** l;

is just the integer sequence A025591 and $M_n = \sqrt{\frac{6}{\pi}} \frac{2^n}{n^{\frac{3}{2}}}(1 + o(1))$. Due to the symmetry, $|S_{\min}|$ is also bounded by M_n. The values of M_n for $n \leq 18$ together with the their ratio to 2^n are listed in Table 4. It is worth noting that $\lim_{n\to\infty} \frac{M_n}{2^n} = 0$, which shows the scale of the simplified inequalities is ignorable with respect to that of the original inequalities. Therefore Algorithm 1 can output a best FLIIC far faster than the common method for a given set $S \in \mathbf{P}^*_{n,+}$.

Table 4. The upper bound of the size of S_{max} (S_{min})

n	1	2	3	4	5	6	7	8	9
M_n	1	1	2	2	3	5	8	14	23
Per (%)	50.00	25.00	25.00	12.50	9.38	7.81	6.25	5.47	4.49

n	10	11	12	13	14	15	16	17	18
M_n	40	70	124	221	397	722	1314	2410	4441
Per (%)	3.91	3.42	3.03	2.70	2.42	2.20	2.01	1.84	1.69

For any $x \in \mathbb{Z}_2^n$, denote

$$\mathrm{succ}(x) = \{u \in \mathbb{Z}_2^n | x \preceq u\}.$$

The following conclusion shows that for any $S \in \mathbf{P}^*_{n,+}$, S can be determined uniquely by $S_{\min}$, where we call $S_{\min}$ the minimal representation of S. Hence we will go through all possible minimal representations directly instead of $S \in \mathbf{P}^*_{n,+}$, which will be used to compute the bound of norms of all linear integer inequalities in Section 4.5.

Theorem 6 (Minimal Representation). *Let $S \in \mathbf{P}^*_{n,+}$. Then we have*

$$S = \bigcup_{x \in S_{min}} \mathrm{succ}(x). \tag{14}$$

Proof: On the one hand, for any $x \in S_{\min}$, note that S is good by Theorem 5, thus $\mathrm{succ}(x) \subseteq S$. So $\bigcup_{x \in S_{\min}} \mathrm{succ}(x) \subseteq S$ holds. On the other hand, for $\forall s \in S$, there exists an $x \in S_{\min}$ such that $x \preceq s$, thus $s \in \mathrm{succ}(x)$. So $S \subseteq \bigcup_{x \in S_{\min}} \mathrm{succ}(x)$. The conclusion follows. □

4.5 Norm and Its Bound

Denote

$$\mathcal{B}_n = \max\{\| S \| \, \big| S \in \mathbf{P}_n\}. \tag{15}$$

In the section we will determine an upper bound of $\mathcal{B}_n$ for a given integer n.

The following theorem gives a bound of $\mathcal{B}_n$ in theory. Due to the limitation of the length of the paper, its proof will be shown in Appendix A.

Theorem 7 (Bound Theorem of Norm). *For any positive integer $n \geq 2$, we have $\mathcal{B}_n < 2^{2n} n!$.*

It can be seen that the above bound in theory is too big and not practical to solve a FLIIC of a given set $S \in \mathbf{P}_n$. Next we will give a tight bound for $n \leq 8$.

A simple method is to go through all $S \in \mathbf{P}_n$ and get the norm of each S. However, $|\mathbf{P}_n|$ is very big and it is hard to go through all plain sets in $\mathbf{P}_n$. Actually, we find that a suitable subset of $\mathbf{P}_n$ is enough to determine $\mathcal{B}_n$, which we will illustrate next.

Lemma 5. *Let $0 \in S \in \mathbf{P}_n \setminus \{\varnothing, \mathbb{Z}_2^n\}$. Then $\| S \| \leq \| \overline{S} \|$.*

Proof: We prove it by contradiction. Assume that $\| S \| > \| \overline{S} \|$, and take $l : (a_0, a_1, \cdots, a_{n-1}, b) \in \mathcal{C}(\overline{S})$, where $\| l \| = \| \overline{S} \|$. Since $0 \notin \overline{S}$, thus $b > 0$. Note that

$$\bar{l} : (-a_0, -a_1, \cdots, -a_{n-1}, -b+1) \in \mathcal{C}(S)$$

and $|-b+1| = b - 1 < b$, we have

$$\| S \| \leq \| \bar{l} \| \leq \| l \| = \| \overline{S} \|,$$

which leads to a contradiction. So $\| S \| \leq \| \overline{S} \|$. □

Lemma 6. *Let $0 \notin S \in \mathbf{P}_n \setminus \{\varnothing, \mathbb{Z}_2^n\}$ with type vector c. Then $\| S \| \leq \| c \oplus S \|$.*

Proof: We prove it by contradiction. Assume that $\| S \| > \| c \oplus S \|$, and take $l : (a_0, a_1, \cdots, a_{n-1}, b) \in \mathcal{C}(c \oplus S)$, where $\| l \| = \| c \oplus S \|$. Since c be the type vector of S, then $0 \notin c \oplus S$. Otherwise, we have $c \oplus S = \mathbb{Z}_2^n$, which contradicts with $S \neq \mathbb{Z}_2^n$. Thus $b > 0$ and $a_i \geq 0$ for all i's. Note that l^c :

$$((-1)^{c[0]} a_0, (-1)^{c[1]} a_1, \cdots, (-1)^{c[n-1]} a_{n-1}, b - \sum_{i=0}^{n-1} c[i] a_i)$$

$\in \mathcal{C}(S)$, we have

$$\| S \| \leq \| l^c \| \leq \| l \| = \| c \oplus S \| .$$

A contradiction. So $\| S \| \leq \| c \oplus S \|$. □

Lemma 7. *Let $S \in \mathbf{P}_n \setminus \{\varnothing, \mathbb{Z}_2^n\}$ and σ be a position permutation derived by the order of S. Then $\| S \| = \| \sigma(S) \|$, where $\sigma(S) = \{\sigma(x) | x \in S\}$.*

Proof: For any $l : (a_0, a_1, \cdots, a_{n-1}, b) \in \mathcal{C}(S)$, we have

$$\sigma(l) : (a_{\sigma(0)}, a_{\sigma(1)}, \cdots, a_{\sigma(n-1)}, b) \in \mathcal{C}(\sigma(S)).$$

Thus $\| l \| = \| \sigma(l) \|$, which implies that $\| S \| = \| \sigma(S) \|$. □

By Lemmas 5, 6 and 7, we only need to focus on the bound of norms of all regular plain sets, that is,

Theorem 8. *For any positve integer n, we have $\mathcal{B}_n = \| \mathbf{P}_{n,+}^* \|$, where*

$$\| \mathbf{P}_{n,+}^* \| = \max\{\| S \| \, \big| S \in \mathbf{P}_{n,+}^*\}.$$

Proof: The conclusion follows directly from Lemmas 5, 6 and 7. □

Since each regular plain set is a good set, thus we can go through all regular plain sets in $\mathbf{P}_{n,+}^*$ fast by means of good sets, see Algorithm 2. Besides, by Theorem 6, we also go through all combinations of minimal representations to do it, but here we do not give more details due to the limit of the paper.

Algorithm 2 FindGoodSets(S, t, $\mathbb{S}$): Go through all good sets in $\mathbb{Z}_2^n$

Input: A positive integer n, the initial set $S = \varnothing$, $\mathbb{S} = \varnothing$ and $t = -1$
Output: All good sets $\mathbb{S}$

```
if S = Z_2^n then
    return ;
end if
if S is good then
    S ← S ∪ {S};
end if
for each x in {x ∈ S̄ | x > t}[4] do
    Compute S ← S ∪ {y ∈ S̄ | x ⪯ y};
    Call FindGoodSets(S, x, S);
end for
```

After getting all good sets $\mathbb{S}$, for each $S \in \mathbb{S}$, we call Algorithm 1 to get both its best FLIIC and norm. As results, $\mathcal{B}_n$ $(1 \leq n \leq 8)$ are listed in Table 5.

5 Plain Closure of Sets

5.1 Minimal Plain Closure

In the section we mainly discuss plain closures of a given set $S \in \mathbf{\Pi}_n$. When $S \notin \mathbf{P}_n$, we need more than one inequality to fully characterize it, each inequality

[4] Here we identify an n-bit string x and an integer x by means of the mapping $x \mapsto \sum_{i=0}^{n-1} x[i]2^i$.

Table 5. The experimental results of $\mathcal{B}_n$

n	1	2	3	4	5	6	7	8
$\mathcal{B}_n$	1	2	3	5	9	18	40	105

fully characterizes a plain set containing S. In another word, we need to expand S into different plain sets. The plain sets obtained by expanding S are called plain closures of S.

Definition 17 (Plain Closure). *Let $S \in \mathbf{\Pi}_n$ and $S' \in \mathbf{P}_n$. S' is called a plain closure of S if $S \subseteq S'$.*

It is noticed that $\mathbb{Z}_2^n$ is a plain closure of all S's, thus we call $\mathbb{Z}_2^n$ to be trivial. For any $S' \in \mathbf{P}_n \setminus \{\mathbb{Z}_2^n\}$, we call S' a non-trivial plain closure of S if $S \subset S'$. At most time we are interested in some minimal plain closures of S, which are defined as below.

Definition 18 (Minimal Plain Closure). *Let $S \in \mathbf{\Pi}_n$ and S' be a plain closure of S. S' is minimal if $\nexists S'' \in \mathbf{P}_n$ such that $S \subseteq S'' \subset S'$.*

A natural observation is that a FLIIC of S can be got by collecting the inequalities corresponding to its minimal plain closures. The following theorem guarantees this assertion.

Theorem 9. *For any $S \in \mathbf{\Pi}_n$ and $L \in \mathcal{C}(S)$, there exists a FLIIC L' of S such that $|L| = |L'|$ and for each $l' \in L'$, l' is a minimal plain closure of S.*

Proof: If all l's in L are minimal plain closures of S, then we take $L' = L$. Otherwise, there exists an $l \in L$ such that l is not a minimal plain closure of S. By Definition 18, there exists a minimal plain closure l' of S such that $l' \subset l$. We replace l with l' in L and get L'. Then L' is also a FLIIC of S due to $\overline{l} \subset \overline{l'}$. For each non-minimal plain closure l, repeat the above procedure till all l's are minimal plain closures. The conclusion holds. □

For a given set $S \in \mathbf{\Pi}_n$, below we will start from type vectors of its plain closures and give a deep-first search algorithm, which can output all minimal plain closures of S.

Lemma 8. *For a given set $S \in \mathbf{\Pi}_n$, suppose S' is a minimal plain closure of S with type vector $c \in \mathbb{Z}_2^n$. If $0 \in c \oplus S$, then $S' = \mathbb{Z}_2^n$.*

Proof: Suppose $l : (a_0, a_1, \cdots, a_{n-1}, b)$ is a FLIIC of $c \oplus S'$. By the definition of type vector, it is known that $a_i \geq 0$ for $0 \leq i \leq n-1$. Since $0 \in c \oplus S$, then $b \leq 0$, which implies that all x's belong to l, that is, $l = \mathbb{Z}_2^n$. By Theorem 2, we have $S' = c \oplus l = \mathbb{Z}_2^n$. □

The following theorem can be directly obtained by Lemma 8:

Theorem 10. *Let $S \in \mathbf{\Pi}_n$ and $c \in \mathbb{Z}_2^n$. Then S has a non-trivial minimal plain closure with type vector c if and only if $c \in \overline{S}$.*

For a given set S, by Theorem 10, we know that there are just $|\overline{S}|$ possible type vectors such that their corresponding minimal plain closures are non-trivial. For each non-trivial type vector c, since all coefficients of the FLIICs of minimal plain closures of $c \oplus S$ are non-negative, thus if $e_i \in c \oplus S$, then all x's with $x[i] = 1$ belong to $c \oplus S$. We remove the i-th bit from all x's in $c \oplus S$ and get a lower dimensional set $\hat{S} \in \mathbb{Z}_2^{n-1}$. If

$$(a_0, \cdots, a_{i-1}, a_{i+1}, \cdots, a_{n-1}, b) \tag{16}$$

is a FLIIC of the minimal plain closure of $\hat{S}$, then

$$(a_0, \cdots, a_{i-1}, b, a_{i+1}, \cdots, a_{n-1}, b) \tag{17}$$

is a FLIIC of the minimal plain closure of $c \oplus S$. In order to characterize the above property, we introduce the concept of secondary degeneration.

Definition 19 (Secondary Degeneration). *Let $S \in \Pi_n$ and $c \in \mathbb{Z}_2^n$. We call S be secondary degenerate relatively to c if $e_i \in c \oplus S$ for some i.*

5.2 Algorithm to get all minimal plain closures

For a given set $S \in \mathbf{\Pi}_n$ and a type vector $c \in \overline{S}$, Algorithm 3 adopts the depth-first search method and outputs all minimal plain closures of S with type vector c. Below we give a sketch of Algorithm 3. First we act a shift c on S and get $S' = c \oplus S$. Since all coefficients of the FLIICs of S' are non-negative, we expand S' by adding all elements in $\overline{S'_i}^-$ into S' till $\overline{S'_i}^- = \varnothing$ for all i's and then deal with the degeneration cases. Next, we check whether S' is an ordered set or not by the Order Theorem. If both $\Gamma_{i,j} \setminus \Gamma_{j,i}$ and $\Gamma_{j,i} \setminus \Gamma_{i,j}$ are non-empty for some i, j, we choose one of them and add it into S'. Repeat this process till S' is an ordered set. Let σ be the position permutation derived by the order of S'. Denote $S'' = \sigma(S')$. Then we check the consistent condition in Definition 15 repeatedly, then choose one of those y which leads to contradictions and add it into S'' till S'' is good. Finally, output $c \oplus \sigma^{-1}(S'')$ as a minimal plain closure of S. It should be pointed out that the correctness of Algorithm 3 is based on Theorem 5, and in practice, we mainly use the case $k \leq 4$ to check the consistent condition and construct candidate minimal closures. In this way, all minimal plain closures can be obtained with great probability. Subsequently, further inspection are applied to confirm these sets are plain and the exact number of the minimal closures can be obtained. To improve the efficiency of the process for checking consistent condition, we take the advantage of minimal and maximal representations. In detail, take $k = 2$ for example, it is not necessary to exhaust all possible quartets to test the consistent condition, just checking $x \dot{+} x' \preceq y \dot{+} y'$ for all $x, x' \in S_{min}$ and all $y, y' \in \overline{S}_{max}$ is enough.

Remark 2 (The time complexity analysis of Algorithms 3). In Line 3, S is updated by computing $\overline{S'_i}^-$ and merging it to S iteratively. It indeed adds all

Algorithm 3 Get all minimal plain closures of S with type vector c

Input: A set $S \in \mathbf{\Pi}_n$ and $c \in \overline{S}$
Output: All minimal plain closures of S

Initialize $\mathbb{M} = \varnothing$ and $\mathbb{S} = \varnothing$;
$S' = c \oplus S$;
Expand S' repeatedly by $S' \leftarrow S' \cup \overline{S'}_i^-$ till $\overline{S'}_i^- = \varnothing$ for all i's;
Check the first and secondary degeneration condition for S' and deal with the degeneration case;
Initialize an empty stack ST and push S' into the stack;
while ST is non-empty **do**
  Pop the top element of ST, denoted by S_{top};
  Compute $\Gamma_{i,j}$ and $\Gamma_{j,i}$ of S_{top};
  Collect all pairs (i,j) into Ω such that $\Gamma_{i,j} \nsubseteq \Gamma_{j,i}$ and $\Gamma_{j,i} \nsubseteq \Gamma_{i,j}$;
  if $\Omega = \varnothing$ **then**
    $\mathbb{S} \leftarrow S_{top}$ and guarantee all order sets are minimal;
  else
    Select a pair (i,j) from Ω;
    Compute $S_1 = S_{top} \cup (e_j \oplus \Gamma_{i,j} \backslash \Gamma_{j,i})$ and $S_2 = S_{top} \cup (e_i \oplus \Gamma_{j,i} \backslash \Gamma_{i,j})$;
    Push S_1, S_2 into ST;
  end if
end while
for each $S \in \mathbb{S}$ **do**
  Determine a position permutation σ by S;
  Compute $S \leftarrow \sigma(S)$;
  Compute $S_{\min}$ and $\overline{S}_{\max}$;
  Check the consistent condition in Definition 15 according to $S_{\min}$ and $\overline{S}_{\max}$, and collect all tuples $(y_0, y_1, \cdots, y_{k-1})$ not satisfying the consistent condition into $\mathbb{Y}$;
  if $\mathbb{Y} \neq \varnothing$ **then**
    Search all possible combinations Y such that for each tuple in $\mathbb{Y}$, exactly one of y_i belongs to Y;
    For each combination Y, do $\mathbb{M} \leftarrow \sigma^{-1}(S \cup Y)$;
  end if
end for
Deal with the anti-degeneration operation for each $S \in \mathbb{M}$ if the degeneration operation in Step 4 has been done;
For each $S \in \mathbb{M}$, compute $S \leftarrow c \oplus S$;
return $\mathbb{M}$;

elements in $\overline{S}$ larger than some element S into S in the sense of weak orders. So at most $|S| * |\overline{S}|$ comparisons are needed, which is bounded by 2^{2n-2}.

The loop from Line 6 to Line 17 aims to generate all order sets. To arrange n integers in order, at most $O(n \log n)$ comparisons are needed. Since each comparison may have two results, the size of $\mathbb{S}$ is bounded by $O(2^{n \log n}) = O(n2^n)$. In practice our experiments show that it is far less than $n2^n$. During the generation of each element in $\mathbb{S}$, about $2n \log n$ $\Gamma_{i,j}$'s need to be calculated and updated at most $n \log n$ times. So the complexity of this loop is $O(n2^n(n \log n)^2) = O(n^3 2^n \log^2 n)$.

The minimal (or maximal) representation of S can be calculated in $|S_{min}||S|$ (or $|\overline{S}_{max}||\overline{S}|$), and the check of the consistent condition takes at most $(|S_{min}||\overline{S}_{max}|)^4$ when $k \leq 4$. According to experimental results, we find that both $|S_{min}|$ and $|\overline{S}_{max}|$ are less than 16 at the most time, and only a few out of one million good candidate sets do not satisfy the consistent condition with $k \leq 4$. Hence we take $k = 4$ in Step 22 and finally fix good candidate sets not satisfying the consistent condition in experiments. Then the total time complexity from Line 18 to Line 27 is about $n2^n * 16^8 \approx n2^{n+32}$, where we take $|\mathbb{S}| = n2^n$.

To summarize, the time complexity of Algorithm 3 is about $n2^{n+32}$ when n is not too large. It should be mentioned that this upper bound is rarely reached in practice because we make lots of relaxation during the analysis.

5.3 Comparison with Sun's and Sasaki and Todo's works

In this section we will compare our method with Sun's [Sun21] and Sasaki and Todo's [Udo21]. Generally speaking, we study the relationship between sets, inequalities and inequality coefficients more systematically and more deeply, and present essential properties of plain sets, including type, sparsity, degeneration, order, minimal and maximal element, norm and its bound, etc, and a sufficient and necessary condition characterizing them, which makes our methods more perfect in both theory and implementation.

First of all, though their works also introduced the concept of the order, their order does not take the influence of the inequality coefficients into consideration, and it is indeed a weak order. We synthesize the weak order and the natural order of inequality coefficients, and introduce the concept of strong order, which exposes the essential order property of a plain set and can narrow the space of candidate good sets in Algorithm 3. For more details on the comparison of order, readers can refer to subsection 4.2.

Secondly, as for the SuperBall Approach in [Sun21], Sun's work starts from the shift to the points to be cut, and then introduces the concept of the order. Different from his technical route, we consider all shifts that cover the entire space and then rigorously prove only those centered on points to be cut are non-trivial. As for the construction of inequalities, his approach entirely relies on MILP solvers to solve the optimization problem. However, our method gets the plain closures directly by the sufficient and necessary condition of plain sets, and does not relies on any third-party tools. Thus our algorithm possesses higher efficiency and does with the S-box of larger dimensions.

Thirdly, their two works do not discuss the coefficient of the inequality. The coefficients of inequalities got by MILP tools are often large, but our method can control strictly the range of inequality coefficients. Although no one can assert the specific relationship between the size of coefficients and the efficiency of the MILP solvers, according to our experiments, smaller coefficients tend to speed up the solution.

Finally, as for applications to the S-boxes used in block ciphers, our method can be suitable for S-boxes with higher dimensions. For example, for some S-boxes used in SKINNY128, MISTY-9 and DRYGASCON256, and so on, their methods can not be feasible but we can! What is more, we can get many better solutions than theirs, especially for the high-dimensional S-boxes. For more details, please see Tables 1 and 2.

6 Applications

6.1 S-boxes

The description of finite set can be used to characterize the propagation rules of cryptographic components in many cryptanalysis. We revisit the original problem: the characterization of the Differential Distribution Table (DDT, in short) in differential analysis. When turning to a bit-oriented block cipher, attackers need to take details of S-boxes into consideration. In an MILP model, modeling S-boxes means to characterize the propagations of differentials, this can be done by exploring the DDT of the S-box, which is a $2^n \times 2^n$ table given by:

$$\mathrm{DDT}(a,b) = \#\left\{x \in \mathbb{Z}_2^n \mid S(x) \oplus S(x \oplus a) = b\right\},$$

where a, b represent the input and output differential respectively.

The truncated version of the DDT is denoted as *-DDT [AST+17], where all non-zero entries of the DDT are replaced by 1. Since probabilities of possible transitions are out of concern, modeling *-DDT is enough for our work to model a Boolean function:

$$\begin{aligned} f: \quad & \mathbb{Z}_2^{2n} \to \mathbb{Z}_2 \\ & (x,y) \mapsto \begin{cases} 0, & \text{if } \mathrm{DDT}(x,y) = 0; \\ 1, & \text{otherwise.} \end{cases} \end{aligned} \tag{18}$$

If $f(x,y) = 1$, (x,y) is defined as a possible transition pattern (non-zero entries in the DDT), otherwise it is defined as an impossible transition pattern (zero entries in the DDT). The goal is to model possible propagation patterns and impossible propagation patterns of the DDT of an S-box by linear constraints (i.e., linear inequalities). Then the problem becomes the description of a subset of $\mathbb{Z}_2^{2n}$, i.e., finding a FLIIC for a given subset. We apply Algorithm 5 to the DDT of various S-boxes and get their best FLIICs. The results are summarized in Table 2. Algorithm 5 is implemented by calling Algorithm 3 $|\overline{S}|$ times. Since there are at most 2^n non-trivial types, then the time complexity is bounded by $n2^{3n+33}$. In addition, our algorithm is parallel-friendly with respect to points in $\overline{S}$.

Algorithm 4 Find all the minimal closures of a set S

Input: A set S of all possible propagation patterns
Output: All the minimal closures of S

Initialize $\mathcal{C} = \varnothing$;
for all $c \in \overline{S}$ **do**
    $\mathcal{C} \leftarrow$ All minimal plain closures of S with type vector c by calling Algorithm 3;
end for
return $\mathcal{C}$;

Algorithm 5 Get a best FLIIC of a set S

Input: A set S of all possible propagation patterns
Output: A best FLIIC L of S

Initialize $L = \varnothing$;
Initialize $\mathcal{C} = \varnothing$;
$\mathcal{C} \leftarrow$ All minimal plain closures of S by calling Algorithm 4;
Get a best solution $\mathbb{C}$ by solving the set cover problem for $\mathcal{C}$;
for all $C \in \mathbb{C}$ **do**
    $L \leftarrow$ A best FLIIC of C by calling Algorithm 1;
end for
return L;

6.2 Impossible Differential

In this section we further apply our FLIIC solution on the DDT of the S-boxes to search the impossible differential trails of SPN ciphers. It is noticed that a systematic method to find all impossible differential trails for SPN block ciphers was provided in [HPW22]. Their idea is to partition the whole difference pair space into small disjoint sets, and a core step of their method is solving the MILP models. Since the search space is large, the whole process needs to solve a large amount of MILP models, and the overall search time depends on the solving efficiency of these models. We just replace the FLIIC solution of S-boxes in their models with the one generated by our algorithm and keep anything else unchanged. The experimental results are shown in the Table 6.2. One can be seen that the new FLIIC solution provided by our algorithm can significantly improve the solving efficiency. Moreover, the larger the rounds, the more significant the effect. This is because the effect of a better FLIIC on the scale of the model is more pronounced for larger rounds. It is reasonable to believe that the best FLIIC will help to provide better cryptanalysis at many time.

Acknowledge

This research was supported by National Key Research and Development Project under Grant No. 2018YFA0704705 and CAS Project for Young Scientists in Basic Research (Grant No. YSBR-035).

Table 6. Comparison of the time of impossible differential trail searches on Skinny-64

Round	Prev. Time	Ours Time	$\frac{T_{ours}}{T_{prev}}$
11	16662 s	6901 s	41.4%
12	19742 s	6294 s	31.2%
13	26186 s	7041 s	26.9%

[1] Prev. Time: The total solving time using the FLIIC of Skinny-64's S-box provided in [HPW22], and the cardinality of their solution is 34;
[2] Our Time: The total solving time using the FLIIC of Skinny-64's S-box provided by our new algorithm, and the cardinality of our solution is 14.

References

AST+17. Ahmed Abdelkhalek, Yu Sasaki, Yosuke Todo, Mohamed Tolba, and Amr M Youssef. Milp modeling for (large) s-boxes to optimize probability of differential characteristics. *IACR Transactions on Symmetric Cryptology*, pages 99–129, 2017.

BBS99. Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 12–23. Springer, 1999.

BC20. Christina Boura and Daniel Coggia. Efficient milp modelings for sboxes and linear layers of spn ciphers. *IACR Transactions on Symmetric Cryptology*, pages 327–361, 2020.

BHMSV84. Robert K Brayton, Gary D Hachtel, Curt McMullen, and Alberto Sangiovanni-Vincentelli. *Logic minimization algorithms for VLSI synthesis*, volume 2. Springer Science & Business Media, 1984.

Bih94. Eli Biham. New types of cryptanalytic attacks using related keys. *Journal of Cryptology*, 7(4):229–246, 1994.

BR11. Andrey Bogdanov and Vincent Rijmen. Zero-correlation linear cryptanalysis of block ciphers. *IACR Cryptology ePrint Archive*, 2011:123, 01 2011.

BS91. Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosystems. *Journal of CRYPTOLOGY*, 4(1):3–72, 1991.

CHP+17. Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. A security analysis of deoxys and its internal tweakable block ciphers. *IACR Transactions on Symmetric Cryptology*, pages 73–107, 2017.

Cpl09. IBM ILOG Cplex. V12. 1: User's manual for cplex. *International Business Machines Corporation*, 46(53):157, 2009.

Dev20. Sage Developers. Sagemath, the sage mathematics software system (version 9.0). 2020.

ES03. Niklas Eén and Niklas Sörensson. An extensible sat-solver. In *International conference on theory and applications of satisfiability testing*, pages 502–518. Springer, 2003.

FWG+16. Kai Fu, Meiqin Wang, Yinghua Guo, Siwei Sun, and Lei Hu. Milp-based automatic search algorithms for differential and linear trails for speck. In *International Conference on Fast Software Encryption*, pages 268–288. Springer, 2016.

HPW22. Kai Hu, Thomas Peyrin, and Meiqin Wang. Finding all impossible differentials when considering the ddt. *Cryptology ePrint Archive*, 2022.

Inc21. OEIS Foundation Inc. The on-line encyclopedia of integer sequences. *Published electronically at https://oeis. org*, 2021.

Knu94. Lars R Knudsen. Truncated and higher order differentials. In *International Workshop on Fast Software Encryption*, pages 196–211. Springer, 1994.

LWZZ19. Ling-Chen Li, Wen-Ling Wu, Lei Zhang, and Ya-Fei Zheng. New method to describe the differential distribution table for large s-boxes in milp and its application. *IET Information Security*, 13(5):479–485, 2019.

Mat93. Mitsuru Matsui. Linear cryptanalysis method for des cipher. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 386–397. Springer, 1993.

MWGP11. Nicky Mouha, Qingju Wang, Dawu Gu, and Bart Preneel. Differential and linear cryptanalysis using mixed-integer linear programming. In *International Conference on Information Security and Cryptology*, pages 57–76. Springer, 2011.

Opt20. LLC Gurobi Optimization. Gurobi optimizer reference manual. 2020.

Qui52. Willard V Quine. The problem of simplifying truth functions. *The American mathematical monthly*, 59(8):521–531, 1952.

SHW+14. Siwei Sun, Lei Hu, Peng Wang, Kexin Qiao, Xiaoshuang Ma, and Ling Song. Automatic security evaluation and (related-key) differential characteristic search: application to simon, present, lblock, des (l) and other bit-oriented block ciphers. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 158–178. Springer, 2014.

ST17. Yu Sasaki and Yosuke Todo. New algorithm for modeling s-box in milp based differential and division trail search. In *International Conference for Information Technology and Communications*, pages 150–165. Springer, 2017.

Sun21. Yao Sun. Towards the least inequalities for describing a subset in z_2^n. Cryptology ePrint Archive, Report 2021/1084, 2021. `https://ia.cr/2021/1084`.

TIHM18. Yosuke Todo, Takanori Isobe, Yonglin Hao, and Willi Meier. Cube attacks on non-blackbox polynomials based on division property. *IEEE Transactions on Computers*, 67(12):1720–1736, 2018.

TSK+16. Cui Tingting, Chen Shiyao, Fu Kai, Wang Meiqin, and Jia Keting. New automatic search tool for impossible differentials and zero-correlation linear approximations. *SCIENCE CHINA Information Sciences*, 2016.

Udo21. Aleksei Udovenko. Milp modeling of boolean functions by minimum number of inequalities. Cryptology ePrint Archive, Report 2021/1099, 2021. `https://ia.cr/2021/1099`.

XZBL16. Zejun Xiang, Wentao Zhang, Zhenzhen Bao, and Dongdai Lin. Applying milp method to searching integral distinguishers based on division property for 6 lightweight block ciphers. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 648–678. Springer, 2016.

Appendix A The Proof of Theorem 7

Definition A.1. *Suppose S is an n-dimensional Euclidean space. Denote v as a point in S and S' as a subspace of S which does not need to contain the origin.*

If there is a point v' in S' such that $\forall \alpha_1, \alpha_2 \in S'$, $\langle \alpha_1 - \alpha_2, v - v' \rangle = 0$, we say v' is the projection from v to S'. The distance from v to S' is defined as the Euclidean distance between v and v'. Morever, the uniqueness of the projection is easily to verified.

Definition A.2. *Suppose v_1 and v_2 are two points in S, v_1' and v_2' are their projections in a subspace S' respectively. The included angle of v_1 and v_2 about S' is defined as the angle between vectors $\boldsymbol{v_1'v_1}$ and $\boldsymbol{v_2'v_2}$ which is denoted as $\rho(v_1, v_2)$.*

Lemma A.1. *Suppose S_n is an n-dimensional Euclidean space, S_{n-1} and S'_{n-1} are two different $(n-1)$-dimensional subspaces of S_n, then $S_{n-1} \cap S'_{n-1}$ is an $(n-2)$-dimensional subspace of S_n.*

Proof: Since $S_{n-1} \neq S'_{n-1}$, we have $S_{n-1} \cup S'_{n-1} = S_n$, then the dimension of their intersection can be calculated as below:

$$\begin{aligned} & dim(S_{n-1} \cap S'_{n-1}) \\ =& dim(S_{n-1}) + dim(S'_{n-1}) - dim(S_{n-1} \cup S'_{n-1}) \\ =& n-2. \end{aligned}$$

□

Definition A.3. *Suppose S_n is an n-dimensional Euclidean space, S_{n-1} and S'_{n-1} are two different $(n-1)$-dimensional subspaces of S_n. Denote $S_{n-2} = S_{n-1} \cap S'_{n-1}$ and α_0 as the origin of S_{n-2}. Suppose $\{\boldsymbol{e_1}, \boldsymbol{e_2}, \cdots, \boldsymbol{e_{n-2}}\}$ is an orthogonal basis of S_{n-2}, $\boldsymbol{e_{n-1}}$ and $\boldsymbol{e'_{n-1}}$ are vectors added when S_{n-2} is extended to S_{n-1} and S'_{n-1} respectively. The included angle between S_{n-1} and S'_{n-1} is defined as $min\{\rho(\boldsymbol{e_{n-1}}, \boldsymbol{e'_{n-1}}), \pi - \rho(\boldsymbol{e_{n-1}}, \boldsymbol{e'_{n-1}})\}$, where $\rho(\cdot, \cdot)$ is the angle between two vectors.*

Remark 1. For every $\alpha_1 \in S_{n-1} \backslash S_{n-2}$ and $\alpha_2 \in S'_{n-1} \backslash S_{n-2}$, the included angle of α_1 and α_2 about S_{n-2} is either equal or complementary to the included angle between S_{n-1} and S'_{n-1}. It is because that $\boldsymbol{\alpha_1'\alpha_1}$ and $\boldsymbol{\alpha_2'\alpha_2}$ are either in the same direction with $\boldsymbol{e_{n-1}}$ and $\boldsymbol{e'_{n-1}}$ or the contrary, where α_1' and α_2' are the projection of α_1 and α_2 in S_{n-2} respectively.

Definition A.4. *Suppose S_n is an n-dimensional Euclidean space, S_{n-1} is an $(n-1)$-dimensional subspace of S_n and S_{n-2} is an $(n-2)$-dimensional subspace of S_{n-1}. Denote the origin of S_{n-2} as α_0 and $\{\boldsymbol{e_1}, \boldsymbol{e_2}, \cdots, \boldsymbol{e_{n-2}}\}$ as an orthogonal basis of S_{n-2}. The rotation of S_{n-1} about S_{n-2} in S_n is defined as a matrix under the orthogonal basis $\{\boldsymbol{e_1}, \boldsymbol{e_2}, \cdots, \boldsymbol{e_n}\}$ of S_n:*

$$R(\beta) = \begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & cos(\beta) & sin(\beta) \\ & & & -sin(\beta) & cos(\beta) \end{bmatrix} \tag{A.1}$$

, where $\beta \in [-\pi, \pi]$. Use S'_{n-1} to denote $R(\beta)S_{n-1}$, then S'_{n-1} is also an $(n-1)$-dimensional subspace of S_n and $\{\boldsymbol{e_1}, \boldsymbol{e_2}, \cdots, \boldsymbol{e_{n-2}}, cos\beta \boldsymbol{e_{n-1}} - sin\beta \boldsymbol{e_n}\}$ is an orthogonal basis of S'_{n-1}.

Remark 2. β in Definition A.4 can be viewed as the angle in Definition A.3.

Proof: Denote $v = x_1\boldsymbol{e_1} + x_2\boldsymbol{e_2} + \cdots + x_n\boldsymbol{e_n}$ which can also be written as $(x_1, x_2, \cdots, x_n)^T$. Suppose $v' = R(\beta)v$, then the projection from v and v' to S_{n-2} is $v'' = x_1\boldsymbol{e_1} + x_2\boldsymbol{e_2} + \cdots + x_{n-2}\boldsymbol{e_{n-2}}$. Since $\boldsymbol{v''v} = (0, 0, \cdots, x_{n-1}, x_n)^T$ and $\boldsymbol{v''v'} = R(\beta)(0, 0, \cdots, x_{n-1}, x_n)^T$, it is easy to check that the angle between these two vectors is β. □

Remark 3. The rotation in Definition A.4 is ergodic.

Proof: For any $\gamma \in S_n$, there exist $\alpha \in S_{n-1}$, $\beta \in [0, 2\pi]$ such that $R(\beta)\alpha = \gamma$. Denote $\gamma = x_1\boldsymbol{e_1} + x_2\boldsymbol{e_2} + \cdots + x_n\boldsymbol{e_n}$ and $\alpha = x_1\boldsymbol{e_1} + x_2\boldsymbol{e_2} + \cdots + x_{n-2}\boldsymbol{e_{n-2}} + \sqrt{x_{n-1}^2 + x_n^2}\boldsymbol{e_{n-1}}$. The final conclusion can be obtained from the properties of the 2-dimensional plane rotation. □

Definition A.5. *Suppose S_n is an n-dimensional Euclidean space and S_{n-1} is an $(n-1)$-dimensional subspace of S_n, which is also known as the hyperplane. S_n is divided into two disjoint parts according to S_{n-1}. We say α, β are on the different sides of S_{n-1} if and only if $\exists \gamma \in S_{n-1}, t \in (0, 1)$, s.t. $\gamma = t\alpha + (1-t)\beta$.*

Remark 4. Suppose S is a subspace of S_n, for any $\alpha, \beta \in S_n$, the line connecting α and β is either in S or has at most one intersection with S.

Lemma A.2. *Suppose S_k is a k-dimensional Euclidean space, S_{k-1} and S_{k-2} are subspaces of S_k whose dimension are $k-1$ and $k-2$ respectively. S_{k-1} is divided into two disjoint parts A and B according to S_{k-2}. Denote the resulting subspace as S'_{k-1} after conducting a rotation in Definition A.4 on S_{k-1}, then A and B are on different sides of S'_{k-1}. If there exist two points α_1 and α_2 on different sides of S_{k-1}, such that the rotation $R(\beta)$ doesn't meet that two points, then $\beta > 0$ ($\beta < 0$) if α_1 (α_2) is on the same side as A.*

Proof: According to Definition A.5, $\forall a \in A$, $b \in B$, $\exists t \in (0, 1)$, $c \in S_{k-2}$, s.t. $c = ta + (1-t)b$. Since $S_{k-2} \subset S'_{k-1}$, $c \in S'_{k-1}$, then a and b are on different sides of S'_{k-1}. The first part of conclusion follows from the arbitrariness of a and b.

As for the second part, without loss of generality, we can assume that α_1 is on the same side as A after a rotation $R(\beta)$, where $\beta > 0$. Choose $a \in A$ which has the same projection p on S_{k-2} with α_1, the line crossing α_1 and a intersects $R(\beta)S_{k-1}$ at the point c and intersects $R(-\gamma)S_{k-1}$ at the point c', where $\gamma > 0$, we only need to prove that if $c = t_1a + (1-t_1)b$, $c' = t_2a + (1-t_2)b$, $t_1 \in (0, 1)$ then $t_2 \notin (0, 1)$. Consider the plane determined by a, α_1 and p, since

$$R(\beta)S_{k-1} = R(\beta + \gamma)R(-\gamma)S_{k-1},$$

we can get $\angle apc = \beta$, $\angle apc' = \gamma$, $\angle cpc' = \beta + \gamma$ by Remark 2, then the conclusion can be obtained according to the knowledge in plane geometry. □

Definition A.6. *Suppose S_n is an n-dimensional Euclidean space with an origin and an orthogonal basis, a point in S_n is called a lattice if and only if each of its coordinate component is either 0 or 1; a point in S_n is called a quarter-lattice if and only if its coordinate components only take values from $\{0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}, 1\}$.*

Definition A.7. *Suppose S_n is an n-dimensional Euclidean space, a k-dimensional subspace S_k is called a lattice-subspace(quarter-lattice-subspace), if and only if it can be determined by $k+1$ lattices(quarter-lattices) $\{\alpha_0, \alpha_1, \cdots, \alpha_k\}$, i.e.,*

$$\{\boldsymbol{\alpha_0\alpha_1}, \boldsymbol{\alpha_0\alpha_2}, \cdots, \boldsymbol{\alpha_0\alpha_k}\}$$

are linearly independent as vectors.

Lemma A.3. *Suppose S_n is an n-dimensional Euclidean space with an origin and an orthogonal basis. Denote S_k as a k-dimensional subspace of S_n whose lattices are divided two parts denoted as A and B by a $(k-1)$-dimensional subspace S_{k-1}. Then S_{k-1} can be mapped to a lattice-subspace S'_{k-1} by some rotations in Definition A.4 without across any lattice.*

Proof: Denote the set of all lattices in S_{k-1} as T_0, define $rank(T_0)$ to be the dimension of subspace V_0 which is determined by T_0. It is clearly that $0 \leqslant rank(T_0) \leqslant k-1$, and we can extend T_0 according to the following operations:

1. While $rank(T_0) < k-1$
2. Choose a $(k-2)$-dimensional subspace V'_0 of S_{k-1} which contains V_0;
3. For every lattice $\alpha \notin T_0$, denote V_α as the subspace which are determined by V'_0 and α, then calculate the included angle between V_α and S_{k-1}. Denote β as the smallest of these angles, let β correspond to lattice α', perform a rotation on S_{k-1} about V'_0 in S_k with angle $\beta' = \beta$ or $-\beta$ such that $\alpha' \in R(\beta')S_{k-1}$.
4. S_{k-1}=$R(\beta')S_{k-1}$;
5. T_0=$\{lattices \ \ in \ \ S_{k-1}\}$.

Since $rank(T_0) < k-1$, we can always find a lattice $\alpha \notin T_0$ and then extend T_0 according to α. The program terminates only if $rank(T_0) = k-1$. Moreover, these operations will never across any lattice since the rotation angle is the smallest of all the lattices. □

Lemma A.4. *Suppose S_n is an n-dimensional Euclidean space with an origin and an orthogonal basis. Denote S_k as a k-dimensional subspace of S_n whose lattices are divided two parts denoted as A and B by a $(k-1)$-dimensional subspace S_{k-1}. Then there exists a $(k-1)$-dimensional quarter-lattice-subspace S'_{k-1} which divides all lattices in S_k into two parts A and B.*

Proof: We fix n and prove the result by induction on k. The conclusion obviously holds when $k = 2$. Assume that the result holds when $k < m-1$.

Suppose $k = m$, then we have an $(m-1)$-dimensional subspace S_{m-1} of S_m which divides all lattices in S_m into A and B. By Lemma A.3, it can be mapped

to a lattice-subspace S'_{m-1}. All lattices in S_m are divided into three parts A', B' and C' where $A' \subset A$, $B' \subset B$, $C' \subset S'_{m-1}$. If $C' = \varnothing$, then S'_{m-1} is exactly what we want. Otherwise, if $C' \neq \varnothing$, consider $S_{m-2} = S_{m-1} \cap S'_{m-1}$ which is a $(m-2)$-dimensional subspace of S'_{m-1} according to Lemma A.1. Then all lattices in S'_{m-1} are divided into two parts A'' and B'' by S_{m-2}, where $A'' \subset A$, $B'' \subset B$. By induction assumption, there exists an $(m-2)$-dimensional quarter-lattice-subspace S'_{m-2} which divides all lattices in S'_{m-1} into A'' and B''. For every lattice $\alpha \notin S'_{m-1}$, calculate the included angle between V_α and S'_{m-1}, where V_α is determined by S'_{m-2} and α, every α corresponds to an angle β and a rotation $R(\beta)$ or $R(-\beta)$. Then we choose $R(\beta_1)$ and $R(-\beta_2)$ among all of these rotations such that their absolute values are the smallest in the two classes respectively.

By Lemma A.2, A'' and B'' will be separated by the rotation $R(\beta)$, and we can choose β_1 or $-\beta_2$ such that A'' is on the same side as A'. Without loss of generality, assume that $R(\beta_1)$ is selected where β_1 corresponds to lattice α'. Consider lattice-subspace S'_{m-1} which is determined by m lattices:

$$\{\alpha_0, \alpha_1, \cdots, \alpha_{m-1}\},$$

choose a lattice $\alpha_i \in S'_{m-1} \backslash S'_{m-2}$, then S'_{m-1} can also be determined by α_i and S'_{m-2}. Denote the quadrisection of $\alpha_i\alpha'$ as $\{\alpha^1, \alpha^2, \alpha^3\}$, according to Remark 4, $\alpha_i\alpha'$ has at most one intersection with S'_{m-2}. So we can choose α^j such that S'_{m-2} and α^j can determine an $(m-1)$-dimensional quarter-lattice-subspace of S_m. Now it only needs to check whether $\rho(\alpha_i, \alpha^j) < \rho(\alpha_i, \alpha')$ holds. Since $\alpha_i, \alpha^j, \alpha'$ are collinear, their projections on S'_{m-2} are collinear, then the question is transformed to a 3-dimensional geometry question which is obviously right. □

Theorem A.1. *Suppose S_n is an n-dimensional Euclidean space with an origin and an orthogonal basis, S_{n-1} is a hyperplane which divides lattices in S_n into two parts A and B. Then there exists another hyperplane S'_{n-1} which can be denoted as $\sum_{i=1}^{n} a_i x_i = d$, a_i, $d \in Z$, and S'_{n-1} also divides lattices in S_n into A and B and $max\{|a_i|, |d|\} < 2^{2n} n!$.*

Proof: By Lemma A.4, there exists a quarter-lattice-subspace S'_{n-1} which divides all lattices in S_n into A and B. S'_{n-1} is determined by $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ where α_i is a quarter-lattice for $1 \leq i \leq n$, plug α_i into S'_{n-1}, $\sum_{i=1}^{n} a_i x_i = d$, we get

$$\begin{aligned} &\left(a_1\ a_2 \cdots\cdots a_n\right)\left(\alpha_1\ \alpha_2 \cdots\cdots \alpha_n\right) \\ =&\left(d\ d \cdots\cdots d\right). \end{aligned}$$

Denote $M = \left(\alpha_1\ \alpha_2 \cdots\cdots \alpha_n\right)$. Then $\left(a_1\ a_2 \cdots\cdots a_n\right) = \left(d\ d \cdots\cdots d\right) M^{-1}$

Since α_i is a quarter-lattice, we have $4M \in M_n(Z)$ and $M^{-1} = 1/4^n (4M)^{-1}$. Then

$$\begin{aligned} &\left(a_1\ a_2 \cdots\cdots a_n\right) \\ =&\left(d\ d \cdots\cdots d\right)\frac{1}{4^n}(4M)^{-1} \\ =&\left(d\ d \cdots\cdots d\right)\frac{1}{4^n|4M|}(4M)^{*}. \end{aligned}$$

Since $0 \leq 4m_{i,j} \leq 4$, one can easily check that $|4M| < 4^n \times n!$. Similarly, for every $m^*_{i,j} \in (4M)^*$, we can get $|m^*_{i,j}| < 4^{n-1} \times (n-1)!$.

Let $d = 4^n|4M| < 4^{2n}n!$, then $\begin{pmatrix} a_1 & a_2 & \cdots & \cdots & a_n \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & \cdots & 1 \end{pmatrix} (4M)^*$. Hence $a_i < n \times 4^{n-1} \times (n-1)! < 2^{2n}n!$ holds for $1 \leq i \leq n$. □